



甲子光年
JAZZY YEAR

2020年

甲子光年智库-信息安全系列研究报告 第一期 信息安全总览及Web应用安全研究报告

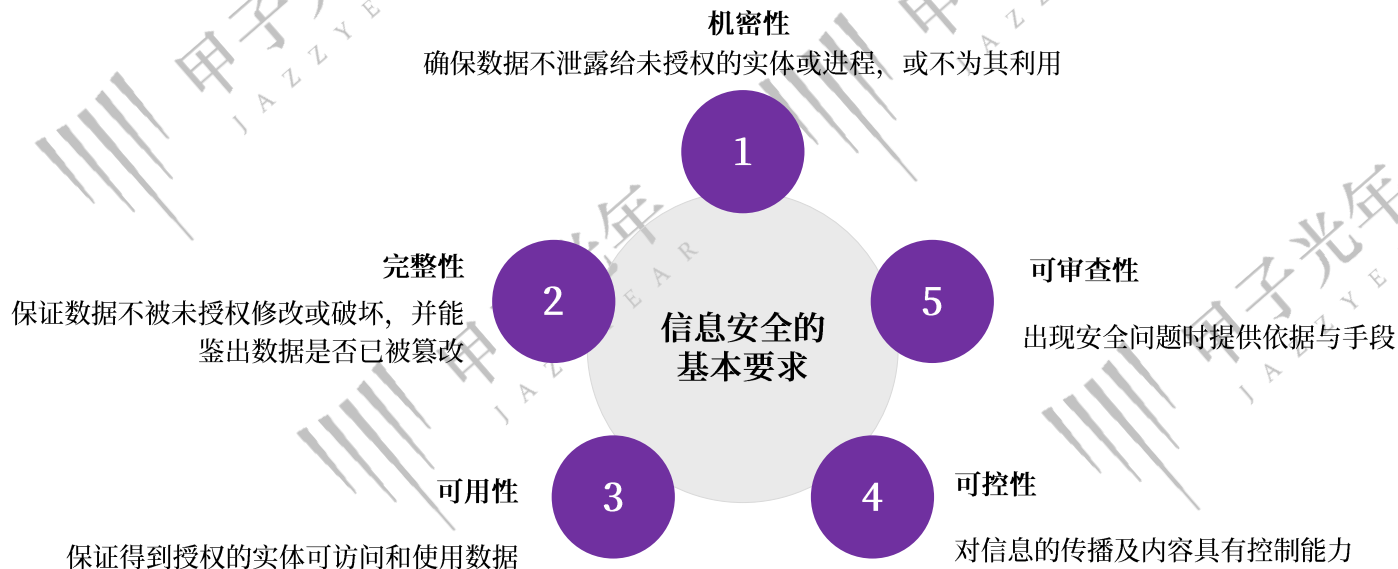
2020年10月

October, 2020

VISIT...

LANZAROTE
Caliente.COM

- 信息安全是指采取技术和管理的安全保护手段，保护各类信息资源中的硬件、软件、通信网络、服务、数据等组成部分，保证各类信息设施正常运作，使其免受各种类型安全威胁的干扰和破坏，确保信息的机密性、完整性、可用性、可控性和可审查性



报告框架

FRAME

1

信息安全总览

信息安全市场发展现状

现代企业信息安全体系

信息安全细分领域供应商

2

重点安全领域介绍之 Web应用安全

Web应用安全的定义

安全威胁分析

安全产品介绍

案例剖析

未来发展趋势



甲子光年

JAZZ YEAR

01

PART ONE

信息安全总览



甲子光年

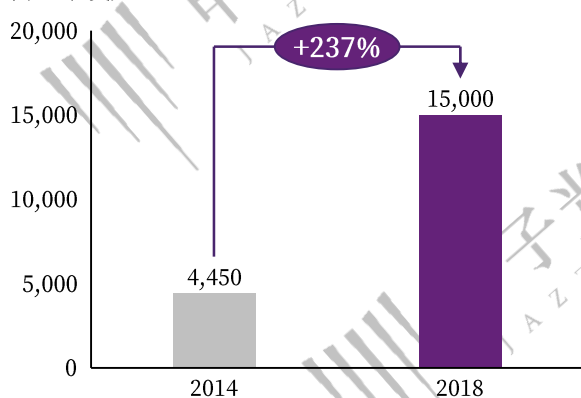
J A Z Z Y E A R

信息安全的重要性日益凸显

- 随着信息化建设的逐步推进，企业的核心业务越发依托信息系统，数据已成为企业的核心资产。新兴技术的不断涌现使得企业自身业务越发依赖于互联网，安全风险也随之上升。信息安全正在成为企业的普适性设施

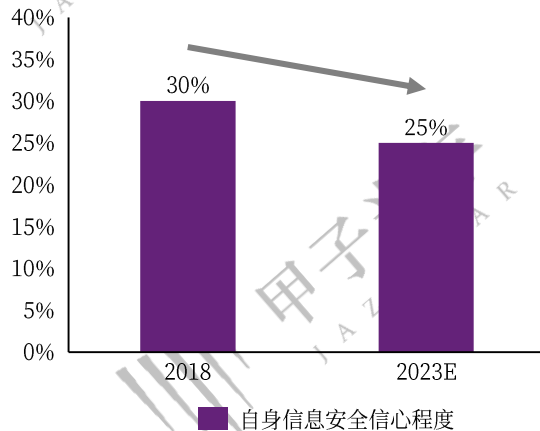
由于网络安全建设不足，网络犯罪造成的损失一直上涨

单位：亿美元



2018 年全球网络犯罪造成的损失达 15000 亿美元，4年之内增加了237%，网络犯罪未能得到有效遏制

绝大部分企业对自身信息安全信心不足

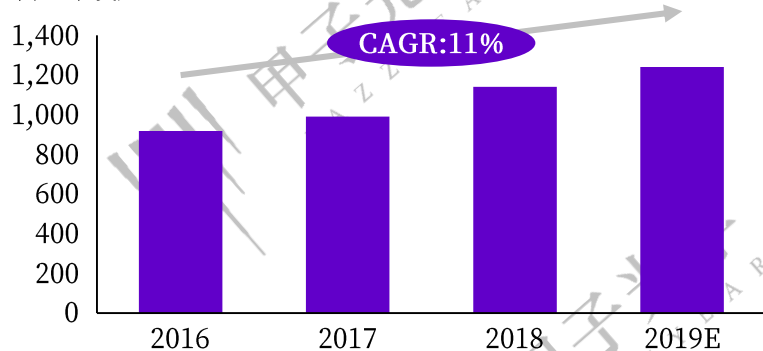


仅有 30%的企业对自身信息安全抱有信心，而且这一数据还在下降，预计五年后将降到 25%

我国信息安全市场目前正在高速增长

全球信息安全市场规模及复合增速

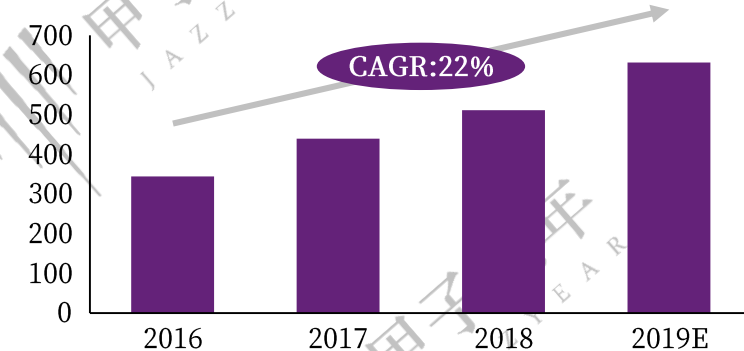
单位：亿美元



预计2019年全球信息安全市场市场规模为**1240亿美元**，近四年复合增速为**11%**，处于快速增长状态中

中国信息安全市场规模及复合增速

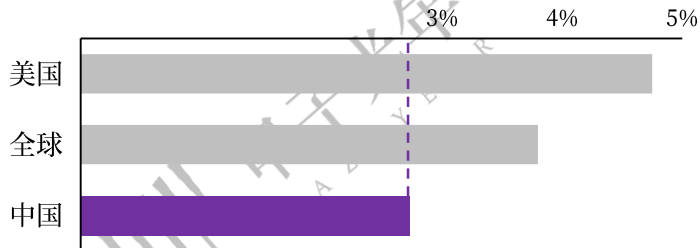
单位：亿人民币



预计2019年我国信息安全市场规模可达**631.29亿元**，近四年复合增速高达**22%**，同全球平均水平相比，我国市场具有巨大的发展潜力

我国信息安全建设水平和发达国家有明显差距

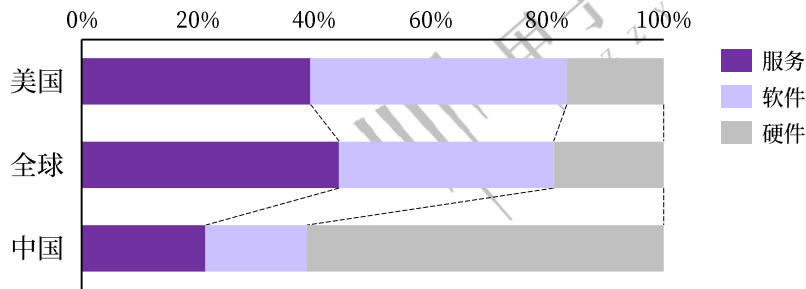
信息安全投入占IT投入的比重



我国信息安全投入在IT投入中占比偏低：

我国信息安全发展起步较晚，企业安全意识较为薄弱，对比全球和美国安全投入水平，我国信息安全渗透率差距明显，安全市场具有极大的增长空间

信息安全投入的构成

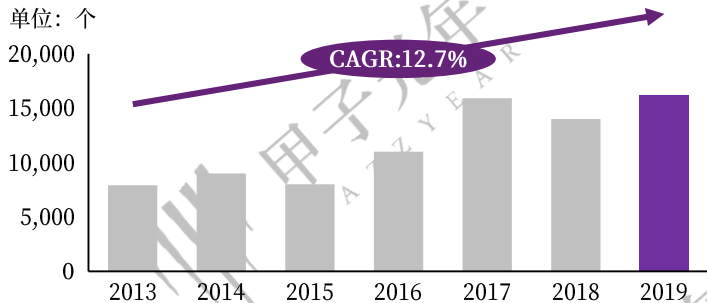


我国缺乏对安全服务和软件的重视：

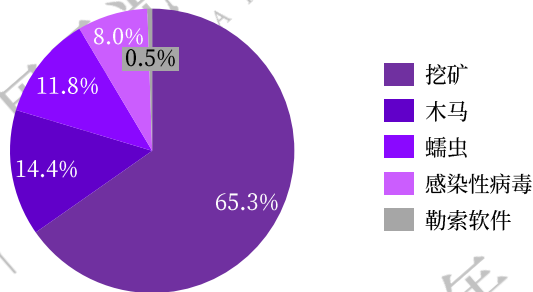
对比全球和美国发展情况，我国硬件占比偏高，企业对作为安全核心的服务和软件的价值认识不足，距离领先的安全建设体系尚有差距

企业面临的威胁和风险不容小觑

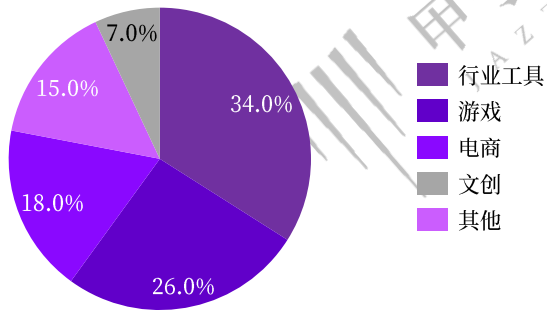
漏洞数量快速增长，2019年创下新高



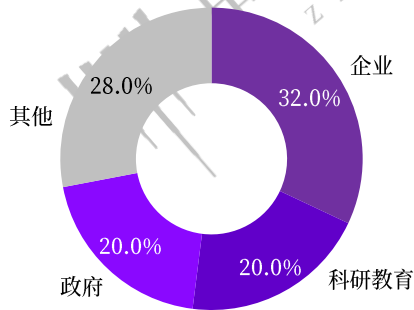
挖矿类和木马类恶意程序是企业终端最大威胁



行业工具、游戏、电商遭受DDoS攻击最多

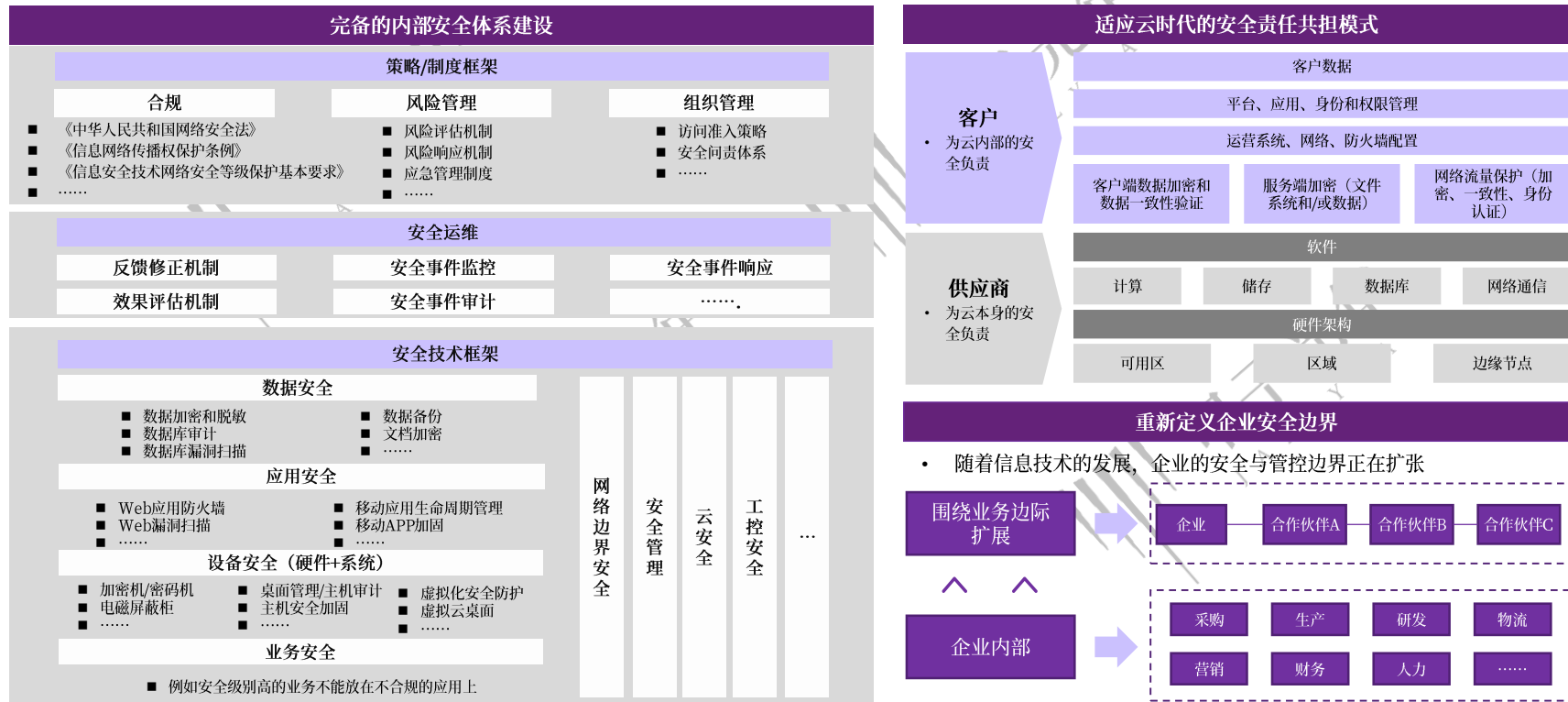


大型企业成为APT（高级持续威胁）的主要攻击目标之一



现代企业需要建立适应云时代发展的“大安全”体系

□ 为满足云时代的安全需求，现代企业需要建立由内部安全体系、安全责任共担和新安全边界三部分构成的“大安全”体系



数据安全细分领域供应商

数据库安全

• 数据库的安全防护

数据库防火墙 	数据库审计 
数据库系统备份 	数据库漏洞扫描 
数据库脱敏 	数据库加密 
数据库运维内控 	

其他数据安全

• 其他各类数据安全防护工具

文档加密 	虚拟机备份与恢复 
数据防泄漏 	数据备份 
数据恢复 	大数据保护 
数据清除工具 	

设备安全细分领域供应商

物理安全

- 设备的实体安全

存储介质信息消除/粉碎机



加密机/密码机



电磁屏蔽柜



红黑电源滤波插座



终端安全

- 终端设备接入网络后的安全

桌面管理/主机审计



源代码加密及嵌入式开发源代码加密



网络防病毒



终端登录/身份认证



补丁管理



单机防病毒



主机安全加固



主机文档加密与权限控制/HDLP



移动存储介质管理



打印安全/打印管理/打印审计



移动及虚拟设备安全

- 移动设备和虚拟设备相关安全防护

虚拟化安全防护



虚拟云桌面



移动终端管理/EMM/MDM



移动统一管理平台



手机防病毒



移动通信安全



应用安全和管理细分领域供应商

Web应用安全

- 用户可以通过浏览器访问的应用程序的安全

网页防篡改	Web应用防火墙	WEB漏洞扫描
网站安全监测产品	网站安全监测服务	网站数据恢复
数据防火墙	应用统一身份管理/身份认证/单点登录/认证网关	半自动&自动化渗透平台
代码审计	加密安全设备/NDLP	反钓鱼/反欺诈

移动应用安全

- 移动设备上运行的应用的安全

安全管理

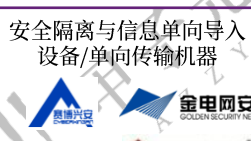
- 支撑信息安全管理工作的各类工具

日志管理/日志审计/SOC/安管平台	运维审计/4A/堡垒机
网络和主机基线配置核查系统	主机安全保密检查工具
应急处置工具	风险评估/安全服务/应急响应
网管软件/ITIL/运维管理系统	漏洞扫描与管理/远程安全评估
信息安全等级保护测评工具箱	网络安全态势感知

网络边界安全细分领域供应商

网络边界安全

• 企业内网的安全检测与边界防护

防火墙/UTM/安全网关 	网络入侵检测NIDS/网络入侵/防御NIPS 	无线入侵检测/防御 	VPN 	上网行为管理 
网络流量控制 	网络流量分析 	防病毒网关/防毒墙 	APT未知威胁发现 	抗DDoS产品和服务 
网闸 	安全隔离与信息单向导入设备/单向传输机器 	网络缓存加速产品及服务 	网络安全审计 	网络准入控制 
负载均衡 	DNS安全 	不良信息识别与监测 	DDI (DNS/DHCP/IP地址管理) 	应用交付 

云安全和工控安全细分领域供应商

云安全

- 随着云技术的发展出现的安全领域

云端DDoS防护 	云端Web应用防火墙 	云安全管理平台 
云主机安全 	云防火墙 	安全云 
微隔离 	容器安全 	
堡垒机 	云端身份管理 	

工控安全

- 工控相关硬件、软件、网络、数据的安全

工控安全网关 	工业防火墙 
工业主机防护系统 	工控脆弱性扫描 
工控态势感知 	工控流量分析/审计 
工控入侵检测 	

不充分的企业安全体系建设可能会引发安全问题

存在缺陷的内部安全体系

- 企业重点安全领域的安全防护建设不足，缺乏有效安全手段，没有能力应对黑客的攻击

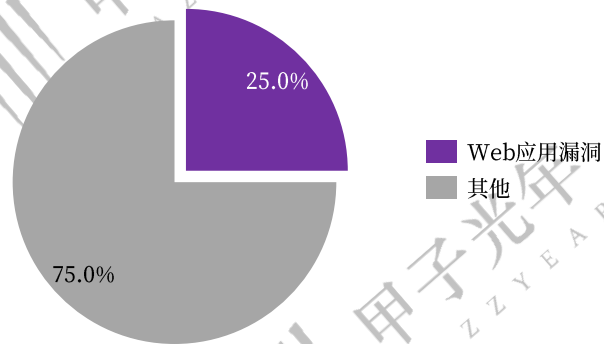
没有意识到需要共担的安全责任

- 企业缺乏责任共担意识和能力，没有同供应商建立有效的合作，不能充分保障关键点复杂、威胁多种多样的云的安全

安全边界仅局限于企业内部

- 企业没有有效扩展安全边界，合作伙伴遇到的安全威胁渗透至企业

云上攻击类型分布



统计数据显示，在云上攻击中，针对Web应用漏洞的攻击占比高达25%，是企业需要重点关注的安全领域之一

02

PART TWO

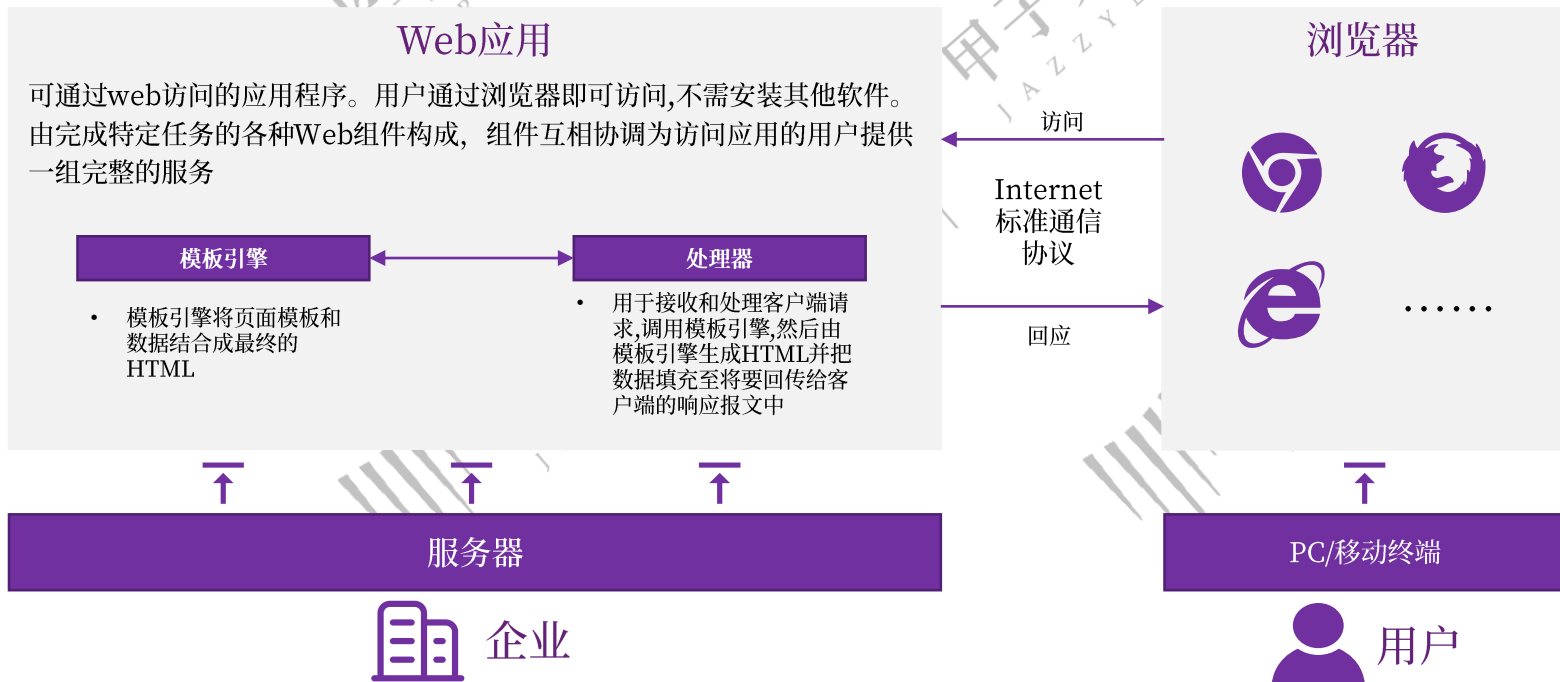
重点安全领域介绍之Web应用安全



甲子光年

J A Z Z Y E A R

- Web应用安全是指用ASP、PHP、JSP、Python等计算机语言编写的Web应用程序及与其相关环境（包括代码、相关数据等）形成的统一的整体所出现的安全问题



等保2.0标准对Web应用的安全要求

- 满足合规性需求是驱动我国企业安全投入的主要因素。2019年5月发布的《信息安全技术网络安全等级保护基本要求》（简称等保2.0标准），**将等级保护制度上升到法律层面，同时将体制外的企业纳入保护对象**
- Web应用适用于等保2.0标准中对应用层面安全的要求，需要注重安全防护的领域梳理如下

入侵防范

- 恶意代码防范
- 接入方式的安全
- 端口与服务的安全
- 漏洞的安全

访问控制

- 用户权限管理
- 账户管理
- 权限策略
- 主客体安全标记

安全审计

个人信息保护

身份鉴别

- 访问者身份唯一
- 密码复杂度
- 登录失败处置
- 远程接入采用加密传输
- 两种以上身份鉴别方式

数据安全

- 数据完整性、保密性
- 数据备份恢复
- 剩余信息保护

Web应用的安全威胁时刻存在

2020年初至今：

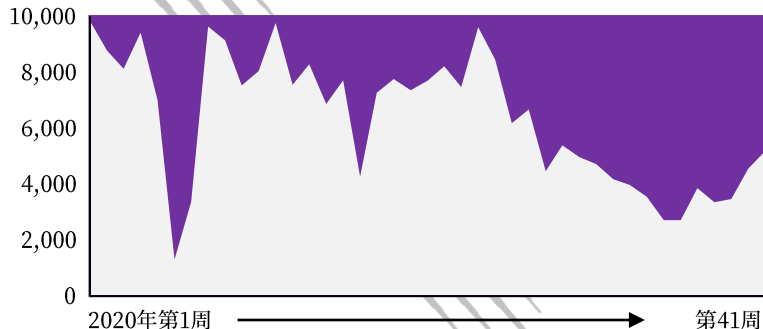
发现Web应用漏洞总数
4580个

平均每周公布Web应用漏洞
117个

单周公布Web应用漏洞最多
338个

Web应用漏洞是黑客攻击时可以利用的Web应用存在的缺陷，每一个漏洞都可能引发潜在的安全风险。Web应用漏洞的修复和完善的过程是持续进行的，企业需要时刻关注

境内被篡改网站总数

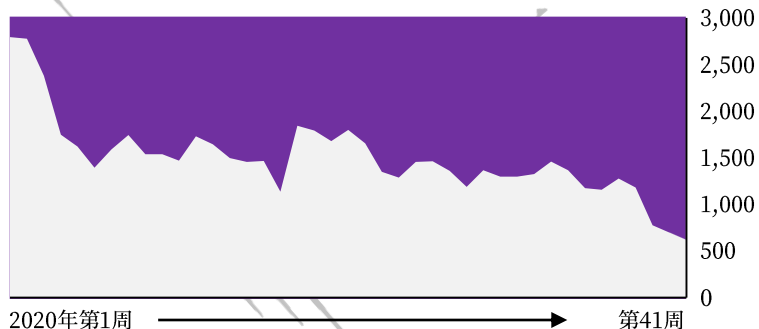


企业

VS

黑客

境内被植入后门网站总数



被篡改和被植入后门的网站往往意味着黑客攻击已经得手，可能对所有者和用户造成巨大损失。围绕Web应用的安全攻防战不曾间断。企业只有提升Web应用安全能力，才能在黑客攻击面前游刃有余

Web应用的安全问题大多由漏洞引起，被攻击后可能产生严重后果

问题存在的原因



Web应用 自身存在漏洞

重大漏洞一旦被黑客利用，可能导致Web应用彻底沦陷，2019年重大漏洞应急响应高达**27次**



开发时期形成漏洞

- Web应用程序的编写人员，在编程的过程中没有考虑到安全的因素，使得黑客能够利用这些漏洞发起对网站的攻击，比如SQL注入、跨站脚本攻击等



系统底层存在漏洞

- Web系统包括底层的操作系统和Web业务常用的发布系统，本身存在诸多的安全漏洞，利用这些漏洞，会给入侵者可乘之机



运维管理中存在漏洞

- 业务系统中由于管理的问题也存在诸多安全隐患，如弱口令、管理员界面等等，导致黑客可以利用这些缺陷进行攻击

遭受攻击

产生的后果

法律风险

被监管强制关站

- 之前某网站被美国反共黑客组织入侵，该公司网页logo和内容被恶意修改，导致网站被封停

经营者承担法律责任

- 网安法规定，网站运营者如果没有履行安全保护义务，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款

经济风险

直接经济损失

- 黑客可能通过修改支付接口，利用拖库信息诈骗客户等方式造成公司的直接经济损失

关键词排名下降

- 网站被挂暗链或木马后，其搜索引擎排名也会受到影响

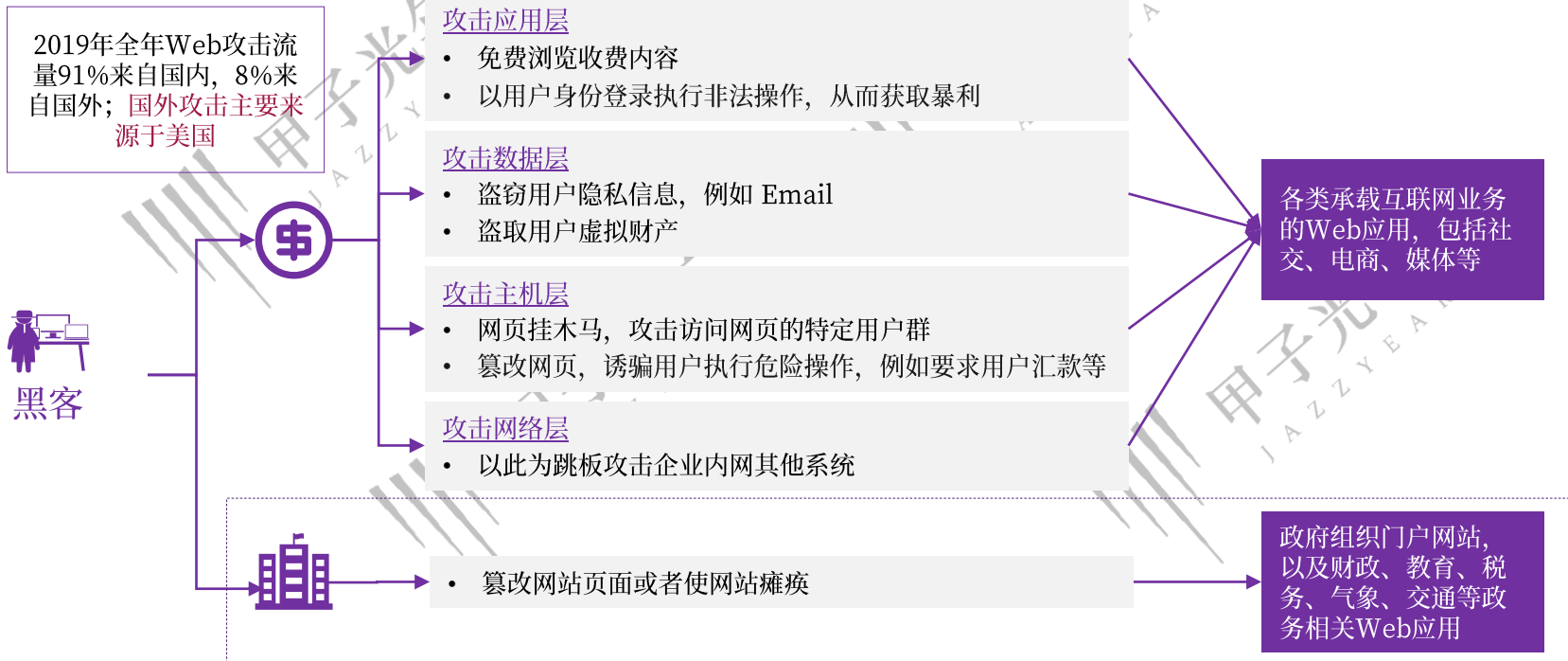
网站被提示不安全

- 用户很可能打开网站即显示不安全，造成网站访问量急剧下降

Web应用攻击主要受经济利益驱动，部分国外攻击具有政治目的

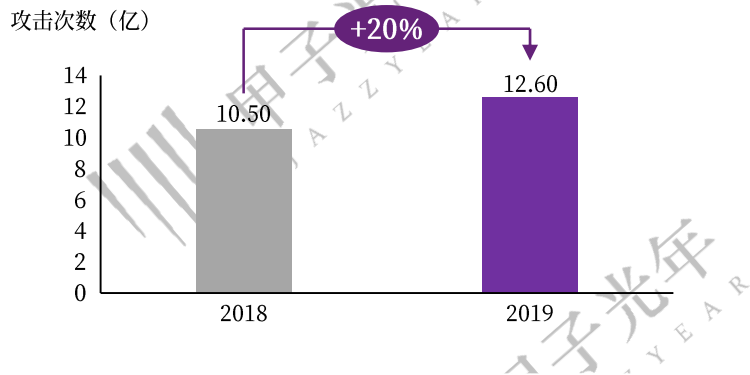
攻击目的

攻击对象



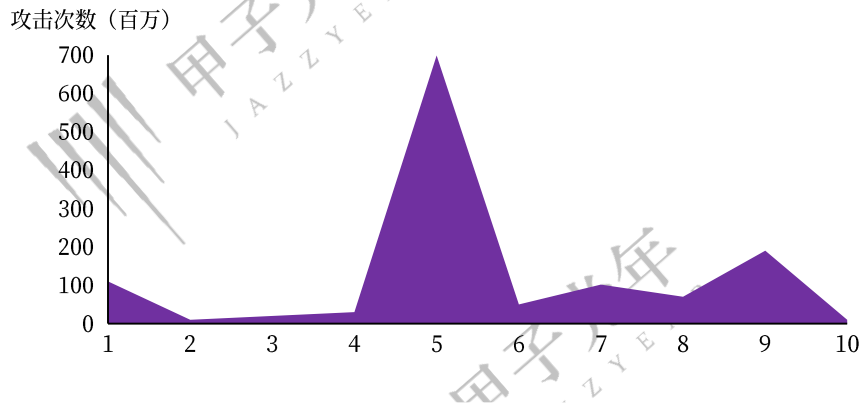
Web应用攻击数量和危害程度均在增加

2019年vs2018年Web应用攻击数量趋势图



同2018年相比，2019年Web攻击数量呈上升趋势，表明Web应用安全形势日益严峻

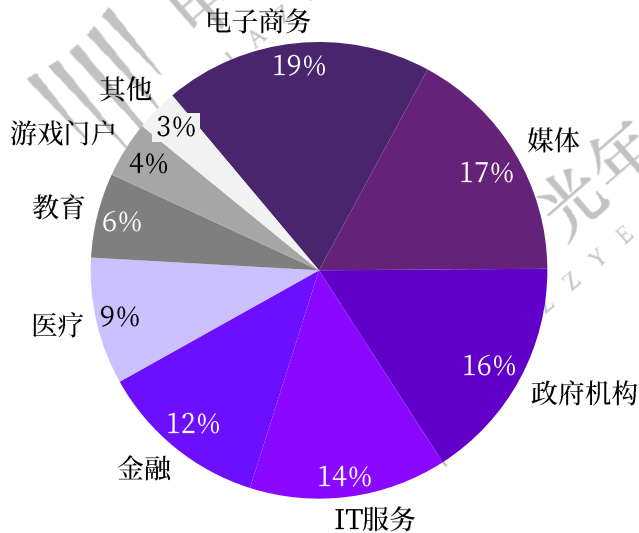
2019年Web应用攻击危害程度分布图



将Web攻击危害从无明显影响(1档)至无法正常运行(10档)划分10个等级，2019年形势表明危害程度呈现出向高转移的趋势

- ▣ 电子商务、媒体、政府机构、IT服务、金融5个行业承载着大部分Web应用访问请求，最受黑客及网络黑产行业的窥视，是攻击流量最为集中的行业

2019年Web攻击行业分布图



什么样的行业尤为需要重视应用安全？



Web应用是企业开展业务的核心途径



用户基数大，群体广



Web应用数据库中储存有大量的用户敏感信息



Web应用数据库中储存有大量的业务相关数据

常见Web应用安全隐患现象与危害程度

业务出现问题

- 促销、抢购等业务活动被黄牛党操纵，普通用户难以参与
- 大量外部爬虫从网站上爬取信息，对用户的正常业务访问请求产生不利影响

应用出现问题

- 用户账户存在安全风险，例如被撞库、虚假注册
- Web应用不断遭受黑客各种攻击行为，出现业务中断等安全事件

数据库出现问题

- 发生数据攻击和泄露事件，用户个人隐私数据被黑客利用

内网出现问题

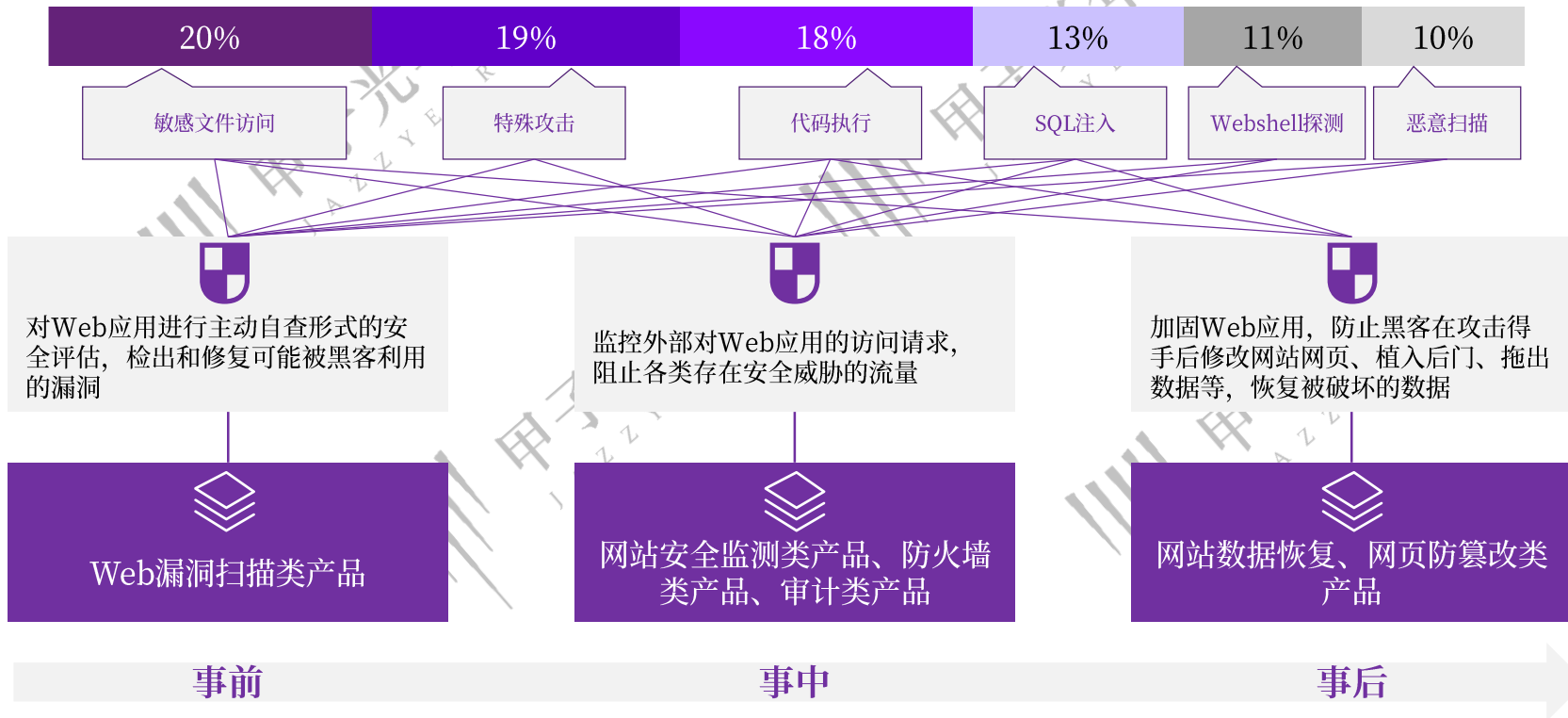
- 内网服务器收到黑客攻击



危害程度

Web应用安全产品的防护思路及类型

2019年主要Web应用攻击类型及分布



Web应用安全主要供应商

目前应用安全领域发展相对成熟，各个领域供应商均可提供较为完善的产品、服务及解决方案

综合供应商



Web漏洞扫描



网站安全监测



代码防火墙



Web应用防火墙



加密安全设备/NDLP



数据库防火墙



网站数据恢复



网页防篡改



半自动&自动化渗透平台



应用统一身份管理/身份认证/单点登录



代码审计



反钓鱼/反欺诈



典型案例剖析：通过全生命周期方案，解决Web应用安全问题（1/2）



案例背景

客户是一家快速发展的国内信托公司

- Web应用是业务发展的重要支撑平台：随着国内信托业务的快速发展，客户广泛使用了互联网门户网站系统、信托业务交易系统等Web应用
- 高数据安全性要求：信托公司托管的是第三方的资产，对数据的完整性、保密性等要求很高，如果内部数据被窃取，将造成很严重的后果

安全防护需求分析

合规需求：

满足相关法律法规的安全防护要求

业务需求：

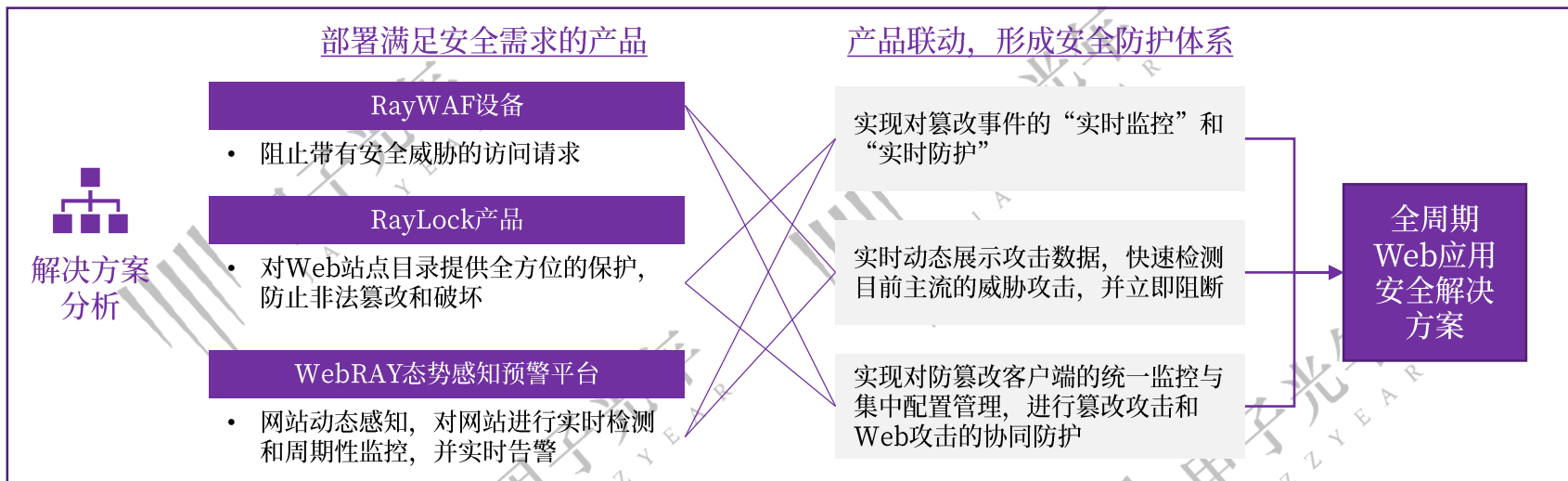
确保业务应用能够快速、安全、可靠地交付

具体需求分析

- 1 具备Web应用威胁全面检测和防护能力
- 2 攻击实时检测和周期监控并及时推送告警
- 3 针对核心Web服务器的漏洞攻击检测与防御
- 4 实时监控网站安全状态，包括是否存在挂马，暗链，钓鱼等威胁
- 5 对互联网访问的网站页面实现防篡改以及具备篡改恢复机制

典型案例剖析：通过全生命周期方案，解决Web应用安全问题（2/2）

甲子光年
JAZZYEAR



Web应用安全未来发展趋势：满足云时代的安全需求

- 随着云计算的广泛应用，越来越多企业将Web应用部署在云端。企业对云基础设施缺乏控制，而供应商提供的配置工具功能有限，云端的安全需要依赖合作伙伴。为此，企业需要和供应商一同探索如何建立有效的安全责任共担模式，保障Web应用的安全



客户

云“内”安全

企业负责管理操作系统、应用程序软件以及防火墙的配置等应用层面的安全，包括：

- 检查和修复Web应用漏洞
- 配置云端Web应用防火墙等防护产品
- 业务系统及发布系统的配置和管理
- 数据的储存、加密
-



企业

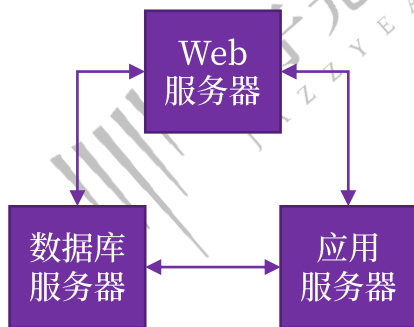
云“自身”安全

供应商负责运行所有云服务的基础设施（硬件、软件、网络和设备）等安全，包括：

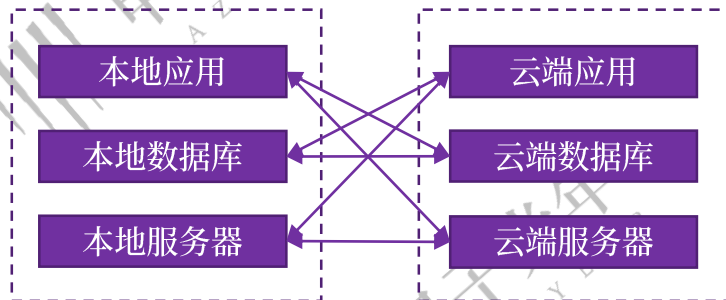
- 确保Web应用的底层设施不存在安全漏洞
- 保护Web应用的底层设施不受到外部攻击
- 确保Web应用的底层设施不会受到非授权访问
- 保证云设施的正常运作
-

Web应用安全产品发展趋势：提升API防护能力

- 随着互联网Web应用技术的发展，API也逐渐被用于来连接Web应用服务和传输数据，成为了现在乃至未来Web应用技术的主流。Web应用从层次明显的架构向多种不同架构混合构成发展，更灵活和敏捷，但是数据安全性降低。确保Web应用中的API的安全需要得到企业和第三方供应商的重视



传统Web应用架构



通过API连接

Web应用安全产品发展方向

- 根据企业实际情况，有针对性地提供用于Web应用连接的API的安全防护能力

Web应用安全产品发展趋势：提升防火墙的智能程度

- Web应用防火墙是Web应用安全的核心产品之一，核心指标是漏报率和误报率。漏报低代表着防护效果好，误报率低则是为了将对正常业务的影响降到最低。面对越来越多样化和复杂的客户业务场景，**标准化和人为更新的防护规则显然不能满足安全防护需求**，厂商正在尝试引入智能技术，突破传统产品在降低漏报和误报上遇到的瓶颈



Web应用安全产品发展趋势：提升对机器流量威胁的安全防护能力

- ❑ 恶意机器流量不断演化，随着新兴技术和新兴工具的使用，以及真人行为操作获取难度的降低，有效区分真实用户流量和恶意机器流量成为企业的难题

恶意机器流量	含义	黑客应用自动化技术，通过调用数据库、伪造键鼠操作、自动输入验证码等手段，绕过或通过Web应用对用户的验证手段，模拟真实用户访问网站，参与业务活动
	危害表现	黑客伪造真实用户的请求，以高速刷量的形式爬取数据、抢购促销商品、抢票、发出虚假订单、垃圾注册、发帖、投票，甚至暴力破解、撞库等，通过黑灰产获利，给企业造成巨大损失
	形势	机器流量正进一步向着技术垂直化、分工明确化、攻击精细化方向发展，下游黑灰产市场对机器流量需求变大，机器流量对抗不断升级

Web应用安全产品发展方向

- 有效识别和阻断技术不断升级的恶意机器流量

名词	释义
漏洞	漏洞是指信息系统中的软件、硬件或通信协议中存在缺陷或不适当的配置，从而可使攻击者在未授权的情况下访问或破坏系统，导致信息系统面临安全风险
恶意程序	恶意程序是指在未经授权的情况下，在信息系统中安装、执行以达到不正当目的的程序
挖矿	占用受害者的系统资源或网络资源进行挖矿，获取加密货币牟利的恶意程序
木马	以盗取用户个人信息，甚至是远程控制用户计算机为主要目的的恶意程序。由于它像间谍一样潜入用户的电脑，与战争中的“木马”战术十分相似，因而得名木马
蠕虫	能自我复制和广泛传播，以占用系统和网络资源为主要目的的恶意程序
病毒	通过感染计算机文件进行传播，以破坏或篡改用户数据，影响信息系统正常运行为主要目的的恶意程序
勒索软件	通过绑架用户文件，使用户数据资产和计算机资源无法正常使用，以此为条件向用户勒索钱财的恶意程序
DDoS（分布式拒绝服务攻击）	多个攻击者（或者一个攻击者通过多台机器）同时向某一目标信息系统发送密集的攻击包，或执行特定攻击操作，以期致使目标系统停止提供服务
APT（高级持续威胁）	由国家背景的相关攻击组织进行攻击的活动，主要通过向目标计算投放特种木马，实施窃取国家机密信息、重要企业的商业信息、破坏网络基础设施等活动，具有强烈的政治、经济目的
网页篡改	恶意破坏或更改网页内容，使网站无法正常工作或出现黑客插入的非正常网页内容
网站后门	黑客在网站的特定目录中上传远程控制页面，从而能够通过该页面秘密远程控制网站服务器
爬虫	按照一定的规则，自动地抓取网页内容和数据的程序或者脚本

信息安全总览及Web应用安全（本期报告）

- 信息安全总览
- 重点安全领域介绍之Web应用安全

终端安全（待发）

- 安全威胁分析
- 安全产品形态分析
- 典型案例剖析
- 未来发展趋势

云安全（待发）

- 安全形势分析
- 安全威胁分析
- 安全产品分类介绍
- 典型案例剖析
- 未来发展趋势

数据安全（待发）

- 安全威胁分析
- 重点安全事件分析
- 安全防护思路及产品介绍
- 典型案例剖析
- 未来发展趋势

网络边界安全（待发）

- 安全威胁分析
- 安全防护思路及产品介绍
- 典型案例剖析
- 未来发展趋势

工控安全（待发）

- 安全形势分析
- 政策要求及安全标准分析
- 安全框架及相应产品
- 安全实践案例分析
- 未来发展趋势

谢谢

THANK YOU



北京甲子光年科技服务有限公司是一家科技智库，包含智库、媒体、社群、企业服务版块，立足于中国科技创新前沿阵地，动态跟踪头部科技企业发展和传统产业技术升级案例，致力于推动人工智能、大数据、物联网、云计算、AR/VR交互技术、信息安全、金融科技、大健康等科技创新在产业之中的应用与落地。



<http://www.jazzyyear.com>